

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 770 997 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.05.1997 Bulletin 1997/18

(51) Int Cl.⁶: **G11B 19/02, G11B 20/00**

(21) Application number: **96307662.5**

(22) Date of filing: **23.10.1996**

(84) Designated Contracting States:
DE FR GB

(72) Inventor: **Liebenow, Frank W.**
Greer, SC 29650 (US)

(30) Priority: **27.10.1995 US 549502**

(74) Representative: **Robinson, Robert George**
International Intellectual Property Department,
NCR LIMITED,
915 High Road,
North Finchley
London N12 8QJ (GB)

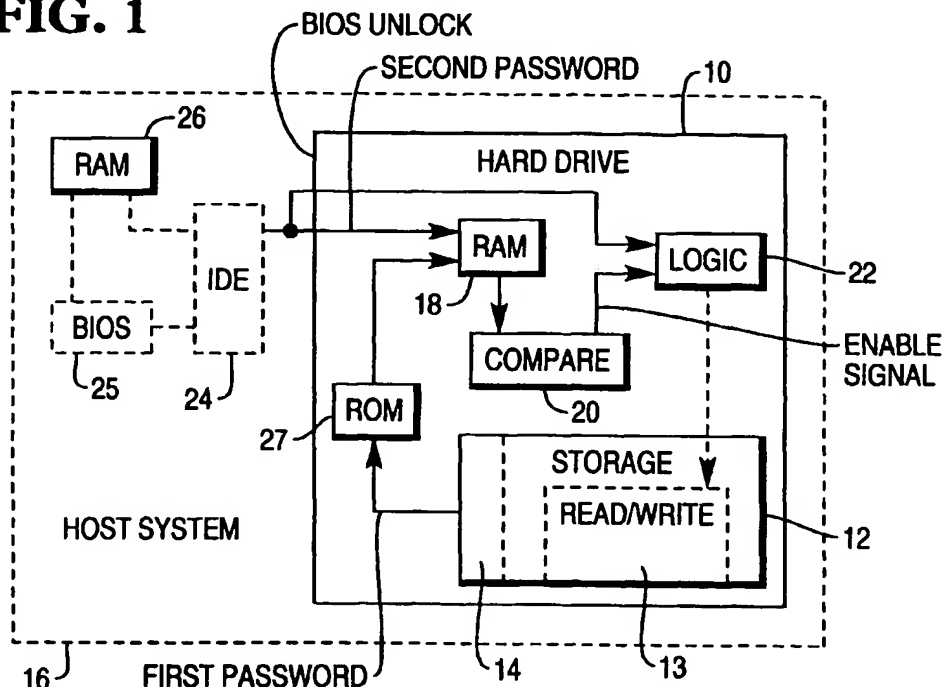
(71) Applicant: **NCR INTERNATIONAL INC.**
Dayton, Ohio 45479 (US)

(54) Password protection for removable hard drive

(57) A device and method for preventing access to data on a hard drive (10) in which a first password is stored (14) on the hard drive so that it is not accessible from a system (16) in which the hard drive is installed, and in which a second password is provided from the

system (16). A comparison of the two passwords is made in a processor (20) in the hard drive to determine whether the two passwords are the same. If the two passwords are not the same, access to the hard drive is denied.

FIG. 1



EP 0 770 997 A2

Description

The present invention relates to methods and devices for controlling access to data, and more particularly to a method and device for preventing unauthorized access to data on a hard drive, regardless of the system in which the hard drive is installed and the password protection available in the system.

As is known, stored data on a data storage device may be protected from unauthorized access in various ways. For example, an operating system program resident in a system in which the data storage device is installed may provide password protection. (The term "password" refers to a sequence of characters in a defined format that is desirably kept secret and used for controlling access to data.) Password protection programs prompt a would-be user to provide a password and deny access unless the user enters a password which matches a predetermined password located in non-volatile memory in the system (i.e. a storage medium which does not lose its contents when system power is removed, such as C-MOS, flash memory, and hard disks). However, these methods are easily bypassed by erasing the non-volatile memory and thus the password protection (e.g. clearing the C-MOS memory by removing the associated battery) or by simply removing the data storage device (e.g. hard drive, floppy disk, PCMCIA memory card, etc.) from the password protected system and installing the data storage device in a non-password protected system.

This problem has been exacerbated by recent technology advances. Data storage devices have become smaller and more easily moved from one system to the next, and many laptop and notebook computers use standard data storage devices, such as Intelligent Drive Electronics (IDE) hard drives, that are purposely engineered to be easily moved from one laptop or notebook computer to the next. It is clearly desirable to provide protection for data stored on a removable data storage device that is independent of the system in which it is installed. It would be a further advantage to be able to use existing technology with only slight modifications to preserve the investments made therein.

Accordingly, it is an object of the present invention to provide a novel device and method for controlling access to data stored on a removable data storage device which obviates the problems of the prior art.

According to the invention there is provided a method of controlling access to data on a removable data storage device, said device being useable in any one of a plurality of systems for processing the data accessed from the data storage device, characterized by the steps of:

- (a) storing a first password on the data storage device so that the first password can be accessed only by the data storage device;
- (b) providing a second password to the data storage

device from a system seeking access to the data on the data storage device;

(c) comparing the first and second passwords on the data storage device; and

(d) permitting access by said system to the data on the data storage device only if the first and second passwords are the same.

The invention will now be described by way of example only with reference to the accompanying drawings in which:-

Figure 1 is a block diagram of an embodiment of the present invention;

Figure 2 is an embodiment of a logic unit of the present invention which provides an access-controlling signal; and

Figure 3 is an embodiment of an access-controlling device in a hard drive of the present invention.

With reference to Figure 1, a hard drive 10 has a storage medium 12 for storing data. The storage medium 12 has a unit 13 for reading and writing data and a predetermined storage location 14 for storing a first password, storage location 14 not being accessible from a host system 16 in which the hard drive 10 is installed. Hard drive 10 also includes a memory (e.g. RAM) 18 for receiving a second password from system 16, a comparator 20 for comparing the first and second passwords and for providing an enable signal when the first and second passwords are the same, and a logic circuit 22 for receiving the enable signal and denying access to storage medium 12 from system 16 in the absence of the enable signal.

Hard drive 10 may include discrete components for accomplishing the functions set forth above, but preferably includes specifically configured firmware in conventional components for accomplishing the functions. System 16, which may be conventional, may optionally include a data request interface 24 (typically an Intelligent Drive Electronics - IDE - interface, although the invention is not limited to IDE devices) for providing a request for access to data on storage medium 12.

By way of further explanation, the first password may be stored in location 14 in storage medium 12 in non-volatile memory. While any number of non-volatile memory options are available and known in the art, preferably the first password is stored on platters (storage media) of the hard drive in a reserved location 14 not accessible from interface 24. This may be accomplished in a manner similar to that currently used by many 2.5" and 3.5" hard drives for storing drive firmware on hidden tracks of the platters. As will be appreciated by those of skill in the art, "hidden tracks" refers to the inability of interface 24 to access the tracks but does not refer to the ability of hard drive 10 to access those tracks.

The presence of a password in storage location 14 provides the initial access control. If a password is found

there, access will not be granted until an enable signal has been provided. If storage location 14 is blank (i.e. does not include a sequence of characters that meets a definition of a password), the hard drive is unprotected and behaves as any other unprotected drive, providing data on request.

An optional BIOS 25 in system 16 may be used to provide the second password to hard drive 10 from interface 24 along with an unlock command. BIOS 25 may prompt the user to enter the second password during power-up. The unlock command informs hard drive 10 that the second password is now available to it, and that it should load the second password into RAM 18 in preparation for the comparison of the two passwords in comparator 20. Currently there is no unlock command in a typical IDE interface command set, and such a command may be added by conventional techniques.

The second password may be stored in a volatile memory 26 in system 16, such as a RAM where stored contents are lost in the absence of power. When access to data on hard drive 10 has been granted and then subsequently denied (e.g. when power to the hard drive is interrupted, such as when the hard drive powers down for energy conservation and the enable signal is lost), the second password must be provided again to the hard drive in order to access data. When power is returned to the hard drive, BIOS 25 checks RAM 26 for the presence of a second password and automatically provides the stored second password to the hard drive for comparison with the first password in the manner described above. Alternatively, BIOS 25 may ask the user to provide the second password each time.

The BIOS 25 may be used to provide a new first password to hard drive 10 through interface 24 with an appropriate command, such as "set password", which tells hard drive 10 to store the new first password in location 14. Once the first password has been stored, data on storage medium 12 cannot be accessed until the BIOS generated unlock command is presented to logic unit 22 from IDE 24 along with the (proper) second password so that the enable signal may be provided.

Comparator 20 in hard drive 10 may compare the first and second passwords to determine whether they are the same. Firmware in a Read Only Memory (ROM) 27 may load the first password into RAM 18, and comparator 20 (e.g. a microprocessor on-board the hard drive) may then compare the first and second passwords from RAM 18. Operation of comparator 20 may be conventional and may be embodied in firmware, with a preferred embodiment including a character-by-character comparison to determine equality. If the two passwords are the same, comparator 20 provides an enable signal to logic unit 22. Further security restrictions may be imposed on the choice of passwords, such as length, and selection of characters that are known to force users to create passwords that are harder to guess.

The operation of logic unit 22 may be understood with reference to Figure 2 which depicts an embodiment

of the unit, although it is to be understood that the logic unit of Figure 2 is but an example and that other embodiments of the logic unit may be used, including firmware in hard drive electronics. An AND gate 30 may receive the unlock signal from BIOS and the enable signal (indicating that the two passwords are the same) from comparator 20. For example, if TRUE is used to indicate access has been requested and permitted, and both inputs to gate 30 are TRUE, the appropriate access-controlling signal may be provided to unlock storage medium 12.

Locking and unlocking of storage medium 14 may be accomplished in several ways. Preferably unauthorized read and write requests may be refused by firmware in hard drive electronics which returns an appropriate error code indicating access has been denied. In a further embodiment of an access-controlling mechanism illustrated in Figure 3, access may be controlled by restricting the flow of data in one or both directions between the drive's read/write head 36 and hard drive electronics 38.

While the foregoing embodiment refers to an IDE interface, the invention may also be used with other types of interfaces, including without limitation a Serial Communication Standard Interface (SCSI), and a Fast IDE Interface. Further, the invention also finds application in data storage devices other than hard drives, and use of the term hard drive herein refers to data storage devices, such as PCMCIA memory cards and the like, which can be adapted to have a "hidden" location for storing the first password and an incorporated data reader for reading the contents of that location so that the first password does not have to be read - and possibly compromised - by the system in which the data storage device is installed.

In a further embodiment of the present invention a fleet password for accessing plural storage media may be used in the same manner as described above. A fleet password may be established and retained by a system administrator to provide an alternative means of accessing data on a restricted storage medium if the above-described second password is lost. A first fleet password common to a plurality of hard drives 10 may be stored in location 14 with the first password and may be compared to a second fleet password in the manner discussed above. For example, logic unit 22 may include an additional AND gate 32 which has as one input the result of the comparison of the first and second fleet passwords and as the other input a BIOS generated unlock signal. The outputs of gates 30 and 32 may be provided to OR gate 34 which provides the appropriate signal to control access to storage medium 12.

In operation, the second password may be compared to the first password, and if it does not match a further comparison may be made to the first fleet password. If the second password matches either, access would be granted.

Claims

1. A method of controlling access to data on a removable data storage device (10), said device being useable in any one of a plurality of systems (16) for processing the data accessed from the data storage device, characterized by the steps of:
 - (a) storing a first password on the data storage device (10) so that the first password can be accessed only by the data storage device;
 - (b) providing a second password to the data storage device from a system (16) seeking access to the data on the data storage device;
 - (c) comparing the first and second passwords on the data storage device; and
 - (d) permitting access by said system to the data on the data storage device only if the first and second passwords are the same,
2. A method according to Claim 1, characterized in that the first password is stored in a predetermined non-volatile storage location (14) in the data storage device (10).
3. A method according to Claim 2, characterized in that the two passwords are compared by the steps of providing the first password from the predetermined storage location (14) in the storage device to a comparator (20) in the data storage device, and comparing the two passwords in the comparator.
4. A method according to Claim 3, characterized in that access to the data is permitted by the steps of providing from the comparator an enable signal if the two passwords are the same, receiving a request for access to the data from the one of the systems, and allowing access to the data in the presence of the enable signal and the request for access.
5. A data storage device (10) removeably installable in a data-access-requesting system (16), said device being characterized by a storage medium (12) having a predetermined storage location (14) for storing a first password, said storage location not being accessible from said system (16),
 - receiving means (18) for receiving a second password,
 - a comparator (20) for comparing said first and second passwords, and for providing an enable signal when said first and second passwords are the same, and
 - logic means (22) for denying access to said storage medium from said system in the absence of said enable signal.
6. A data storage device according to claim 5, characterized in that said storage location (14) further stores a fleet password, whereby when said receiving means (18) receives a second fleet password, said comparator (20) compares said first and second fleet passwords and provides said enable signal when said first and second fleet passwords are the same.
7. A data storage device according to claim 5 characterized in that said logic means (18) comprises a circuit between a read/write head (36) of said data storage device and drive electronics (38) for said data storage device, said circuit comprising a logical gate responsive to said enable signal.
8. A data storage device according to any one of claims 5,6, or 7, characterized by comprising a hard drive.

FIG. 1

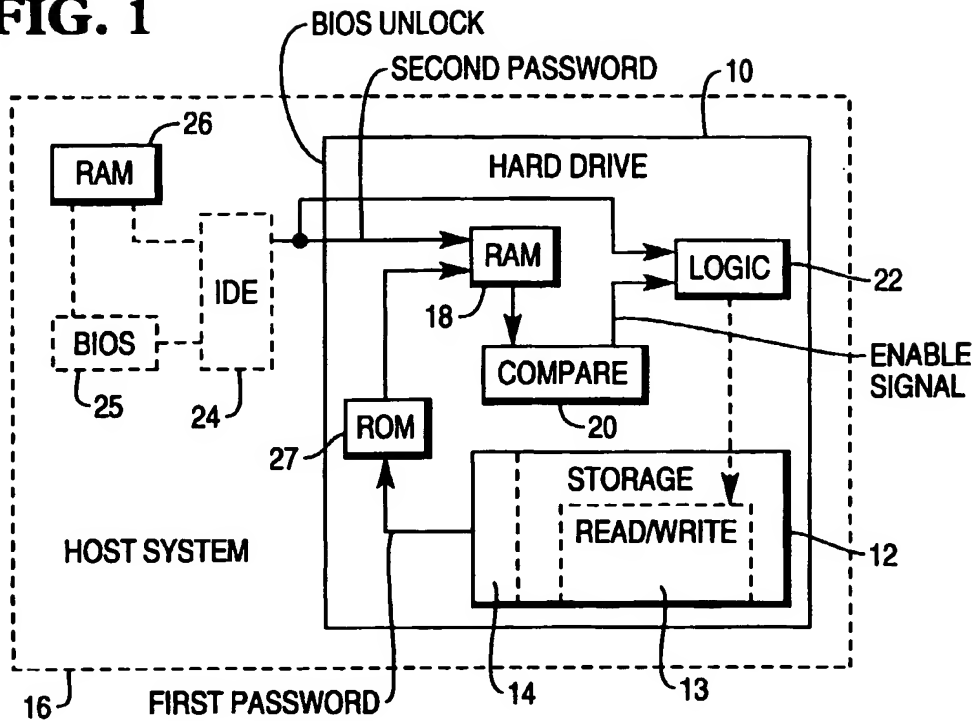


FIG. 2

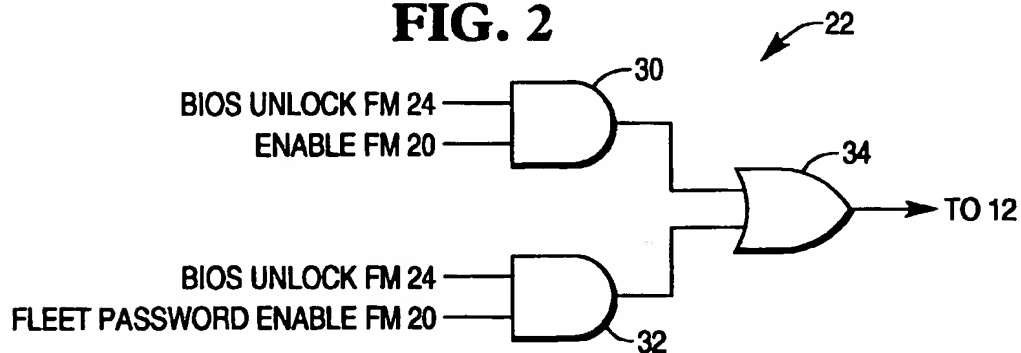


FIG. 3

